

# Informe del Ejercicio Práctico: Escaneo de Subred con Detección de Servicios y Reporte

## 1. Objetivo del Ejercicio:

El objetivo de este ejercicio fue automatizar un escaneo de red sobre una subred local, detectar los servicios que se ejecutan en puertos abiertos, identificar las versiones del software de esos servicios y generar un resumen legible que pueda ser utilizado en un reporte técnico.

## 2. Descripción del Programa:

El script `escaneo_de_red.py` es una herramienta de línea de comandos diseñada para realizar un escaneo de descubrimiento de red utilizando la poderosa funcionalidad de Nmap a través de la librería `python-nmap`. El programa permite al usuario especificar una subred (ej. `192.168.1.0/24`) o una dirección IP específica, para luego escanearla en busca de hosts activos, puertos abiertos y la versión del servicio que se ejecuta en esos puertos. Los resultados se presentan en un formato estructurado y fácil de leer.

## 3. Funcionalidades Implementadas:

- **Integración con Nmap:**

- El script utiliza la librería `python-nmap` para interactuar directamente con la herramienta de escaneo de red Nmap.
- Realiza un escaneo de servicio y versión (`-sV`) en los puertos más comunes (Fast scan `-F`), permitiendo identificar el nombre del servicio y su versión de software.

- **Detección de Hosts Activos y Puertos Abiertos:**

- Identifica todos los hosts que responden en la subred u objetivo especificado.
- Para cada host activo, lista los puertos TCP que se encuentran en estado "abierto".

- **Identificación de Servicios y Versiones:**

- Para cada puerto abierto, el script intenta determinar el nombre del servicio que se ejecuta (ej., `http`, `ssh`) y, si es posible, la versión específica del software (ej., `Apache httpd 2.4.29`, `OpenSSH 7.6`).

- **Generación de Reporte Estructurado:**

- Los resultados se imprimen en la consola de manera organizada, agrupando los servicios detectados por cada host activo.
- Incluye un conteo final del total de hosts activos encontrados.

- **Manejo de Entradas y Errores:**

- Solicita al usuario la subred o IP objetivo a escanear.
- Incorpora manejo de excepciones para errores relacionados con Nmap (por ejemplo, si Nmap no está en el PATH del sistema) y otros errores inesperados, proporcionando mensajes informativos al usuario.

#### 4. Requisitos para la Ejecución:

Para que el script escaneo\_de\_red.py funcione correctamente, es necesario tener instalados:

- **Nmap:** La herramienta de escaneo de red (disponible en [nmap.org](https://nmap.org)).
- **python-nmap:** La librería de Python para interactuar con Nmap (instalable con pip install python-nmap).

```
=== Escáner de Subred y Detección de Servicios ===

Ejemplo de subred: 192.168.1.0/24 o un host específico: 192.168.1.1
Ingresa la subred o IP objetivo para escanear: 192.168.56.1
--- Iniciando Escaneo de Subred en: 192.168.56.1 ---
Esto puede tardar unos minutos, por favor, espera...

--- Resumen del Escaneo de Red ---
Host: 192.168.56.1
- Puerto 135: msrpc(Microsoft Windows RPC )
- Puerto 139: netbios-ssn(Microsoft Windows netbios-ssn )
- Puerto 445: microsoft-ds
- Puerto 5432: postgresql(PostgreSQL DB 9.6.0 or later)

Total de hosts activos: 1
-----
```